(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 September 2001 (07.09.2001)

PCT

(10) International Publication Number
WO 01/65806 A2

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/US01/06598

(22) International Filing Date: 1 March 2001 (01.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/516,410 1 March 2000 (01.03.2000) US

(71) Applicant: SUN MICROSYSTEMS, INC. [US/US]; 901 San Antonio Road, MS UPALO1-521, Palo Alto, CA 94303 (US).

(72) Inventors: HANNA, Stephen, R.; 3 Beverly Road, Bedford, MA 01730 (US). PERLMAN, Radia, J.; 10 Huckleberry Lane, Acton, MA 01720 (US).

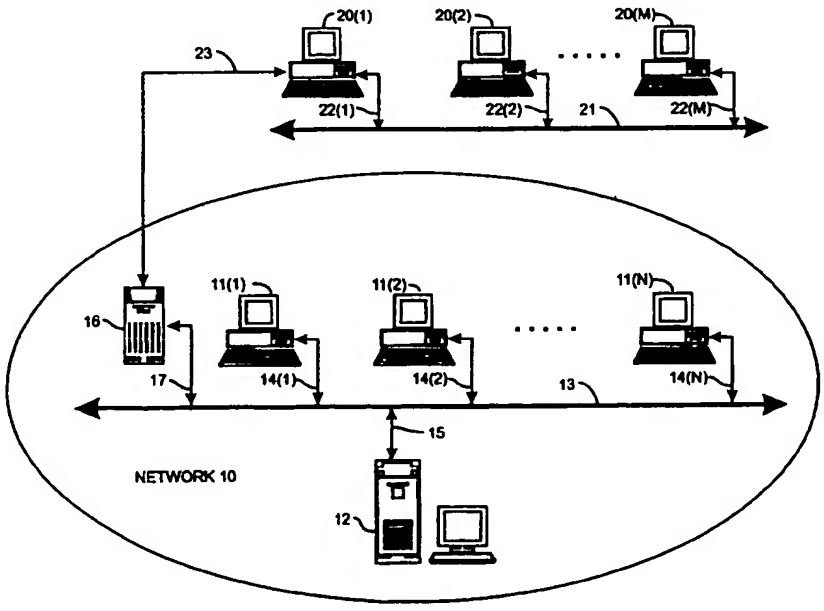
(74) Agents: SORKIN, Paul, D.; Sun Microsystems, Inc., 1 Network Drive, MS UBUR02-310, Burlington, MA 01803 et al. (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR AVOIDING RE-ROUTING IN A COMPUTER NETWORK DURING SECURE REMOTE ACCESS



(57) Abstract: A firewall includes a message packet receiver module and a message packet transfer module. The message packet receiver module receives a message packet to be transferred between a network and a device over a secure connection, the device having a device address. The message packet transfer module selectively transfers the message packet over at least one of the network or the secure connection. In connection with message packets received from the network for transfer over the secure connection, the message packet includes a destination address, and the message packet transfer module is configured to transfer the message packet over the secure connection if the destination address corresponds to the device address of the device, and to not transfer the message packet over the secure connection if the destination address does not correspond to the device address. On the other hand, in connection with message packets received from the secure connection for transfer over the network, the message packet includes a source address, and the message packet transfer module is configured to transfer the message packet over the network if the source address corresponds to the device address of the device, and to not transfer the message packet over the network if the source address does not correspond to the device address. In both cases, the message packet includes a data portion including data, and the firewall may encrypt the data in the data portion in connection with message packets to be transmitted over the secure connection, and decrypt encrypted data in the data portion in connection with message packets received over the secure connection.

WO 01/65806 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR AVOIDING RE-ROUTING IN A COMPUTER NETWORK DURING SECURE REMOTE ACCESS

SYSTEM AND METHOD FOR AVOIDING RE-ROUTING IN A COMPUTER NETWORK DURING SECURE REMOTE ACCESS

FIELD OF THE INVENTION

The invention relates generally to the field of digital computer systems and more particularly to systems and methods for facilitating secure communications over a network or the like. The invention particularly provides an arrangement for avoiding re-routing of message packets by a computer or other device (generally, "computer") that is involved in communications over a secure connection with a second computer, to a third computer connected thereto, and for avoiding re-routing of packets received from the third computer to the second computer over the secure connection.

BACKGROUND OF THE INVENTION

In modern "enterprise" digital data processing systems for use in an office environment in a company, a number of personal computers, workstations, and other various network resources such as mass storage subsystems, network printers and interfaces to the public telephony system, are typically interconnected in a computer network. The personal computers and workstations are used by individual users to perform processing in connection with data and programs that may be stored in the network mass storage subsystems. In such an arrangement, the personal computers/workstations, operating as clients, download the information, including data and programs, from the network mass storage subsystems for processing. In addition, the personal computers or workstations will enable processed data to be uploaded to the network mass storage subsystems for storage, to a network printer for printing, to the telephony interface for transmission over the public telephony system, or the like. In such an arrangement, the network mass storage subsystems, network printers and telephony interfaces operate as shared resources, since they are available to service requests from all of the clients in the network. By organizing the network in such a manner, the servers are readily available for use by all of the personal computers/workstations in the network. Networks may be spread over a fairly wide area, and may interconnect personal computers, workstations and other devices among a number of companies and individuals.

To enhance workers' flexibility, many enterprises allow their employees to work at home or other places not maintained by the enterprise, in addition to or instead of offices or other facilities maintained by the enterprise. To accommodate that, enterprises often allow an employee to connect to their internal networks over external communication links comprising, for example, the Internet or the public switched telephony network (PSTN). Generally, an enterprise connects its internal network to the Internet or PSTN through a "firewall" to protect its internal network from being accessed over the Internet or PSTN by an unauthorized person. A firewall is essentially a computer or other device that connects to both the external communication link and to the internal network and mediates communications therebetween. Essentially, communications are in the form of message packets, and the firewall receives each message packet from the external communication link that is destined for a computer connected to the internal network, determines whether the communication is authorized and, if so, transfers the message packet over the internal network, which, in turn, transfers the message packet to the destination computer. Similarly, the firewall receives each message packet from the internal network that is destined for a computer connected to the external communication link, determines whether the communication is authorized and, if so, transmits the message packet over the external communication link, which, in turn, transfers the message packet to the destination computer. A firewall may determine whether a message packet is authorized by examining address information in the packet, such as its source and/or destination address, a port number or the like.

To ensure that information in message packets transferred over the external communication link is secure in case of interception by a third party, typically communications thereover is in the form of a "secure connection." For a secure connection, information in the message packets transferred over the external communication link will be encrypted using any convenient encryption methodology. Typically at the beginning of a session, a session key will be established between the external computer and the firewall which will be used in encrypting and decrypting information in message packets transmitted therebetween. In that case, the secure connection can be considered as effectively being part of the respective

organization's internal network, and the firewall will normally transfer message packets from the external computer over the internal network (after decrypting the information therein), and message packets from the internal network that are to be transferred to the external computer over the secure connection (after encrypting the information therein).

In such an arrangement, a problem can arise, however, if the external computer is also connected to one or more other computers outside of the enterprise's internal network, and if the external computer is further enabled to operate as a packet router, since typically once a secure connection is set up, the firewall ignores the address information in message packets thereover when performing the transfer. In that situation, if, for example, the computer receives a message packet from the firewall over the secure connection, it may, after the information is decrypted, forward the message packet to the other computer, particularly if the address information in the message packet indicates that the other computer is the destination. Similarly, if the computer receives a message packet from the other computer, it may forward it (that is, the message packet) over the secure connection. Some types of computers will automatically operate as a packet router if they receive message packets from other computers. In any case, the possibility that an external computer might operate as a router can be undesirable, since it can result in the transmission of information received from the internal network over an insecure connection, that is, over the connection between the external computer and the other computer.

SUMMARY OF THE INVENTION

The invention provides a new and improved system and method for avoiding re–routing of message packets by a computer or other device that is involved in communications over a secure connection with a second computer, to a third computer connected thereto, and to avoid re–routing of packets received from the third computer to the second computer over the secure connection.

In brief summary, the invention provides a firewall arrangement for use in connection with a network, the firewall arrangement comprising a message packet receiver module and a message packet transfer module. The message packet receiver

module is configured to receive a message packet to be transferred between the network and a device over with secure connection, the device having an device address. The message packet transfer module is configured to selectively transfer the message packet over at least one of the network or the secure connection. In particular, the message packet transfer module determines whether to transfer the message packet in relation to the device address and an address in the message packet as received by the message packet receiver module.

In particular, in connection with message packets received from the network for transfer over the secure connection, the message packet includes a destination address, and the message packet transfer module is configured to transfer the message packet over the secure connection if the destination address corresponds to the device address of the device, and to not transfer the message packet over the secure connection if the destination address does not correspond to the device address. On the other hand, in connection with message packets received from the secure connection for transfer over the network, the message packet includes a source address, and the message packet transfer module is configured to transfer the message packet over the network if the source address corresponds to the device address of the device, and to not transfer the message packet over the network if the source address does not correspond to the device address. In both cases, the message packet includes a data portion including data, and the firewall arrangement may encrypt the data in the data portion in connection with message packets to be transmitted over the secure connection, and decrypt encrypted data in the data portion in connection with message packets received over the secure connection.

The firewall arrangement can guard against unauthorized routing of message packets to computers which are not part of a secure connection, which may occur if a device with which a secure connection is established is conditioned to operate as a packet router. This will minimize the likelihood that information from the network will be transmitted over insecure connections external to the network. In addition, it will minimize the likelihood of message packets from unauthorized sources external to the network being routed over the network.

BRIEF DESCRIPTION OF THE DRAWINGS

This invention is pointed out with particularity in the appended claims. The above and further advantages of this invention may be better understood by referring to the following description taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a schematically functional schematic diagram of an arrangement including a network and one or more computers located externally of the network, including an arrangement for avoiding re-routing during secure remote access, constructed in accordance with the invention; and

FIGS. 2 and 3 are flow charts depicting operations performed by the network depicted in FIG. 1 in connection with the invention.

DETAILED DESCRIPTION OF AN ILLUSTRATIVE EMBODIMENT

FIG. 1 is a functional schematic diagram including a network 10 and one or more computers, identified by reference numerals 20(1) through 20(M) (generally identified by reference numeral 20(m) located externally of the network 10, and including an arrangement for avoiding re-routing during secure remote access, constructed in accordance with the invention. The network 10 is generally maintained by an enterprise, such as a company or other organization, government agency, or the like, for use by its employees in connection with the business of the enterprise, and will facilitate sharing of information among the employees, while contemporaneously protecting the information from unauthorized access by persons from outside of the enterprise. With reference to FIG. 1, network 10 includes a plurality of computers 11(1) through 11(N) (generally identified by reference numeral 11(n)), 12 and 16 interconnected by a communication link 13. Generally, the computers 11(n) in the network 10 are used by employees of the enterprise and other authorized persons in connection with their work for the enterprise. As is conventional, at least some of the computers 11(n) are in the form of personal computers or computer workstations, each of which includes a system unit, a video display unit and operator input devices such as a keyboard and mouse. The computers 12 and 16 also include a system unit, and may also include a video display

unit and operator input devices. The computers 11(n), 12 and 16 are of the conventional stored–program computer architecture. A system unit generally includes processing, memory, mass storage devices such as disk and/or tape storage elements and other elements (not separately shown), including network interface devices represented by respective arrows 14(n), 15 and 17 for interfacing the respective computer to the communication link 13. A video display unit permits the computer to display processed data and processing status to the user, and an operator input device enable the user to input data and control processing by the computer. The computers 11(n), 12 and 16 transfer information, in the form of message packets, through their respective network interface devices 14(n), 15 and 17 among each other over the communication link 13.

The communication link 13 interconnecting the computers 11(n), 12 and 16 in the network 10 may, as is conventional, comprise wires, optical fibers or other transmission media for carrying signals representing message packets among the computers 11(n), 12 and 16. Alternatively or in addition, the communication link 13 may include one or more wireless links, such as but not limited to an infrared link. The communication link 13 may further include switches for switching signals representing message packets among the computers 11(n), 12 and 16. As noted above, each of the computers 11(n) typically includes a network interface device 14(n), which connects the respective computer to the communications link 13. The transmission media and switches comprising communication link 13 may interconnect the computers 11 in any convenient topology.

Information is transferred among the computers 11(n), 12 and 16 in the form of message packets. Each message packet contains a header portion, which generally contains information that is useful in controlling the transfer of the message packet from the source computer, that is, the computer that transmits the message packet, to the destination computer or computers, that is, the computer or computers that is/are to receive the message packet, and a data portion, which generally contains information that is to be transferred. Generally, any of the computers 11(n), 12 and 16 can operate as a source computer and as a destination computer. The information contained in the header portion includes message packet transfer protocol

information, including, inter alia, source and destination addresses that identify the source computer and the destination computer(s) that is/are to receive the message packet, and each computer can determine from a message packet's destination address whether it is to receive the message packet.

The computers 11(n), 12 and 16 preferably transfer information according to the client–server paradigm. According to that paradigm, certain computer systems in the network, illustratively computer 12, are designated as servers, and other computers, for example, computers 11(n) are designated as clients. The server computer 12 stores information for processing by the client computers 11(n) thereby to enable the client computers to conveniently share the information. A client computer system which needs access to information maintained by a particular server will enable the server to download the information to it over the network. After processing the data, the client computer system may also return the processed data to the server for storage. The computers 11(n), 12 and 16 may also transfer information in message packets in a "peer–to–peer" manner, in which one computer, illustratively computers $11(n_X)$ and $11(n_Y)$ (n_X, $n_Y \in 1,...N$) , exchange information over, for example, a connection established therebetween over communication link 13.

External computers 20(m) may be constructed similar to the various computers comprising the network 10, and may also operate in a similar manner. The external computers 20(m) include network interface devices represented by respective arrows 22(m) for interfacing the respective computer to a communication link 23 to facilitate transfer of information thereamong. In transferring information, the external computers transfer information by means of message packets in a manner similar to the manner in which the computers 11(n), 12 and 16 transfer message packets thereamong over communication link 13.

The computer 16 operates to provide a firewall arrangement permitting communications between the computers in the network 10 and computers which are external to the network 10 which are being operated by authorized individuals, thereby to permit the external computers to access information in the network 10, to retrieve the information from the network 10 and to store processed information therein. In the following, it will be assumed that an authorized individual wishes to

use external computer 20(1) to access information in the network 10. In that operation, the authorized individual, as operator of external computer 20(1), will enable the external computer 20(1) to establish a communications session with the firewall computer 16, which, in turn, mediates communications between the external computer 20(1) and another computer, illustratively server computer 12, in the network. During the communications session, the external computer 20(1) communicates with the firewall computer 16 over a communication link identified by reference numeral 23. Communication link 23 may comprise any convenient communications arrangement, including the Internet, Public Switched Telephony Network (PSTN), or any other form of network or point–to–point connection, or any combination thereof.

Initially during the communications session, the computers 20(1) and 16 will establish a secure connection therebetween using any known technique so that, if a third party attempts to eavesdrop on communications between the computers over the communication link 23, or if a message packet is erroneously received at another computer (not shown), the information contained in the message packet will not be apparent. To avoid that, during a session, the information in the message packets transferred over communication link 23 will be encrypted by the transmitting computer 20(1) or 16, and decrypted by the receiving computer 16 or 20(1), respectively. To facilitate that, in establishing a secure connection, a session key will be generated by one of the computers 20(1) and 16 and provided to the other computer in a conventional manner. When a computer 20(1) or 16 has a message packet to transmit to the other computer 16 or 20(1), it will use the session key to encrypt the information in the message packet before transmitting the message packet to the other computer 16 or 11(1). Since, when the message packets are transferred over the communication link 23, the information in them is encrypted, even if a message packet is received by a third party, the third party will not be able to understand or make use of the information in the message packet.

During a communications session, the external computer 20(1) will operate as a client in a manner similar to the computers 11(n) in the network 10 to retrieve information from the server computer 12 and store information thereon. When the

external computer 20(1) is performing an access operation in connection with the server 12, it will generate a message packet for transfer to the firewall computer 16 over communication link 23, with the information in the message packet being encrypted as described above. If the access operation is to retrieve information from the server 12, the information in the message packet will generally include a retrieval command including an identifier that identifies the information to be retrieved, which retrieval command will, as described above, be encrypted before the message packet is transmitted over communication link 23. The message packet will also include the destination and source addresses as described above, with the source address identifying the external computer 20(1) and the destination address identifying the server computer 12. The source and destination addresses will be unencrypted so that the firewall computer 16 will be able to recognize them without decrypting the message packet. The firewall computer 16 will generally receive the message packet over the communication link 23, decrypt the information in the message packet and transfer the message packet with the decrypted information to the server computer 12. The server computer 12, after receiving the message packet, will obtain the information identified in the retrieval command, generate one or more message packets for transfer to the external computer 20(1) including the information requested by external computer 20(1), and transfer the message packet(s) to the firewall computer 16. In that case, in addition to the information to be retrieved, the message packet(s) will also include the destination and source addresses as described above, with the destination address identifying the external computer 20(1) and the source address identifying the server computer 12. The firewall computer 16, in turn, will receive the message packet(s), encrypt the information therein, and transfer the message packet(s) with encrypted information to the external computer 20(1) over the communication link 23.

On the other hand, if the access operation is to transfer information to the server 12 for storage thereon, the external computer 20(1) will generate one or more message packets containing a storage command and the information to be stored for transfer to the firewall computer 16 over communication link 23. In this case, the storage command and information to be stored will be encrypted, as described above,

before the message packet is transmitted over communication link 23. The message packet will also include the destination and source addresses as described above, with the source address identifying the external computer 20(1) and the destination address identifying the server computer 12. The firewall computer 16 will receive the message packet over the communication link 23, decrypt the storage command and information to be stored in the message packet(s) and transfer the message packet(s) with the decrypted information to the server computer 12. The server computer 12, after receiving the message packet, will store the information as specified in the storage command. Thereafter, the server computer 12 may also provide an acknowledgment message packet to the external computer 20(1) acknowledging that it has received the message packet(s) containing the storage command and information to be stored, and that the information to be stored has been stored. In that case, the server computer 12 will generate the acknowledgment message packet, including the acknowledgment as the information in the packet, and transfer the message packet(s) to the firewall computer 16. The firewall computer 16, in turn, will receive the message packet(s), encrypt the information therein, and transfer the message packet(s) with encrypted information to the external computer 20(1) over the communication link 23. The external computer 20(1) can decrypt the information contained in the message packet to obtain the acknowledgment.

As noted above, a computer, such as external computer 20(1), can be enabled to operate as a packet router. In that condition, external computer 20(1) may forward message packets from another external computer 20(m) ($m \neq 1$) to the firewall computer 16 over the secure connection over communication link 23. Accordingly, if, for example, the external computer 20(2) generates a message packet for transmission to server computer 12, with server computer 12 being identified as the destination computer in the message packet, and external computer 20(2) being identified as the source computer, the external computer 20(2) will forward the message packet to the external computer 20(1) over communication link 21. Thereafter, the external computer 20(1) will forward the message packet to the firewall computer 16 over the secure connection. In that operation, the external computer 20(1) will encrypt the information in the message packet and transmit the

message packet with the encrypted information to the firewall computer 16. When the firewall computer 16 receives the message packet, it would normally decrypt the information and transfer the message packet, with the decrypted information, to the server computer 12.

Similarly, the server computer 12 may generate a message packet for transmission to the external computer 20(2) through the firewall computer 16 and external computer 20(1), the latter operating as a packet router. This may occur if, for example, a message packet transmitted earlier by the external computer 20(2) to the server computer 12 contained a retrieval command. In that case, the server computer 12 will generate one or more message packets containing the information to be retrieved and transfer them to the firewall computer 16. The message packets generated will have identify the server computer 12 as the source computer and the external computer 20(2) as the destination computer. Normally, as with message packets transmitted to the external computer 20(1) as described above, the firewall computer 16 would encrypt the information in the message packets and transfer them to the external computer 20(1) over the secure connection. When the external computer 20(1) receives the message packets, it would decrypt the information and forward the message packets, with the decrypted information, to the external computer 20(2) over the communication link 21.

It will be appreciated that, during such communications between external computer 20(2) and server computer 12 using the external computer 20(1) and firewall computer 16 as intermediaries, the information transferred over the link between the external computers 20(1) and 20(2) generally will not be secure if the connection between external computers 20(1) and 20(2) is not a secure connection. Even if the connection between the external computers 20(1) and 20(2) were a secure connection, the external computer 20(2) may be hostile to the network 10, and so it is generally undesirable to allow external computer 20(1) to be used as an intermediary to transfer information between the external computer 20(2) and the server 12. In accordance with the invention, to minimize particularly the likelihood that information from the network will be transferred between external computer 20(2) and the server 12 using external computer 20(1) as an intermediary, before the

firewall computer 16 transfers a message to the external computer 20(1) over the secure connection over communication link 23, it checks the destination address in the message packet that it receives over the communication link 13 which is to be transferred thereover after the information therein is encrypted, to verify that the destination address is that of the external computer 20(1) for which the secure connection was established. If the destination address in the message packet is that of the external computer 20(1), the firewall computer 16 will proceed to encrypt the information in the message packet and transfer it over the secure connection. On the other hand, if the destination address in the message packet is not that of the external computer 20(1) for which the secure connection was established, the firewall computer 16 will not transfer the message packet (either with the information encrypted or unencrypted) over the secure connection. Instead the firewall computer 16 can discard the message packet. In addition, the firewall computer 16 may provide a notification to the source computer (illustratively, server computer 12) and/or the destination computer (illustratively, external computer 20(2)) indicating, for example, that the information transfer was unauthorized.

In addition, to further isolate the network 10 from unauthorized communications from external computers 20(m) ($m \neq 1$) other than the external computer 20(1) with which the secure connection was established, the firewall computer 16, when it receives a message packet from the external computer 20(1) over the secure connection, will check the source address in the message packet to verify that the source computer was the external computer 20(1). If the firewall computer 16 determines that the source address in the message packet is the address of external computer 20(1), the firewall computer 16 will decrypt the information and forward the message packet, with the decrypted information, to the destination. On the other hand, if the firewall computer 16 determines that the source address in the message packet is not the address of the external computer 20(1) with which the secure connection was established, the firewall computer 16 will not transfer the message packet (either with the information encrypted or unencrypted) over the communication link 13. Instead the firewall computer 16 can discard the message packet. In addition, the firewall computer 16 may provide a notification to the source

computer (illustratively, external computer 20(2)) and/or the destination computer (illustratively, server computer 12) indicating, for example, that the information transfer was unauthorized.

Operations performed by the firewall computer 16 in connection with the invention will be described in connection with FIGS. 2 and 3. FIG. 2 specifically depicts operations performed in connection with message packets that the firewall computer 16 receives from the secure connection, and FIG. 3 depicts operations performed in connection with message packets that the firewall computer 16 receives from the network 10. With reference initially to FIG. 2, when the firewall computer 16 receives a message packet from the secure connection (step 100), it initially determines whether the source address in the message packet corresponds to the source address of the external computer with which the secure connection was established (step 101). If the firewall computer 16 makes a positive determination in step 101, it proceeds to decrypt the information in the message packet (step 102) and transmits the message packet over the communication link 13 connected thereto (step 103), thereby to facilitate transfer of the message packet to the destination computer.

Returning to step 101, if the firewall computer 16 makes a negative determination in that step, which will occur if the source address in the message packet does not correspond to the address of the external computer with which the secure connection was established, it (that is, firewall computer 16) will proceed to step 105, in which it transmits message packets to the source and destination indicating that a source which was not authorized to transfer a message packet over the secure connection had attempted to transfer a message packet thereover. In addition, the firewall computer 16 will discard the message packet (step 106).

With reference to FIG. 3, when the firewall computer 16 receives a message packet from communication link 13 connected thereto (step 110), it initially determines whether the destination address in the message packet corresponds to the destination address of the external computer with which the secure connection was established (step 111). If the firewall computer 16 makes a positive determination in step 111, it proceeds to encrypt the information in the message packet (step 112) and transfer the message packet over the communication link 23 connected thereto (step

113), thereby to facilitate transfer of the message packet to the destination external computer.

Returning to step 111, if the firewall computer 16 makes a negative determination in that step, which will occur if the destination address in the message packet does not correspond to the address of the external computer with which the secure connection was established, it (that is, firewall computer 16) will proceed to step 115, in which it transmits message packets to the source and destination indicating that a source had attempted to transfer a message packet over the secure connection to a destination that was not authorized to receive a message packet thereover. In addition, the firewall computer 16 will discard the message packet (step116).

The invention provides a number of advantages. In particular, it provides an arrangement by which the firewall computer 16 can guard against unauthorized routing of message packets to computers which are not part of a secure connection, which may be accomplished if an external computer, with which a secure connection is established, is conditioned to operate as a packet router. This will minimize the likelihood that information from the network 10 will be transmitted over insecure connections external to the network 10. In addition, it will minimize the likelihood of message packets from unauthorized external sources being routed over the network 10.

It will be appreciated that a number of modifications may be made to the arrangement described above in connection with FIGS. 1 through 3. For example, although the network 10 has been described as comprising various computers (including the above–described server computer 12, client computers 11(n) and firewall computer 16), it will be appreciated that a network may also include, for example, printers and facsimile devices, digital audio or video storage and distribution devices, and the like, which may be shared among the various computers connected in the network 10 and the external computer 20(1).

Furthermore, although the secure connection has been described as being provided by encryption in connection with information transmitted thereover, it will be appreciated that a secure connection can be provided using other conventional

mechanisms. In such cases, the information may be transmitted using plain text, which may be authenticated using any conventional authentication arrangement.

In addition, although the invention has been described in connection with computers 11(n), 12, 16 and 21(m), it will be appreciated that the invention can be used in connection with any type of device which may operate as a source or destination of message packets and which may be connected to either communication link 13, 21or 23, including but not limited to appliances, personal digital assistant devices, and the like.

Furthermore, although the invention has been described in connection with a network 10 in which computers 11(n), server 12 and firewall 16 are separate devices, it will be appreciated that a computer 11(n) may also operate as and perform the functions described above for a server 12 and/or a firewall 16. In that case, for example, hardware and/or software connections may provide information transfer between hardware and/or software components performing operations described above for computers 11(n), server 12 and firewall 16.

In addition, although the firewall computer 16 has been described as sending notifications to the source and destination after it receives unauthorized message packets received from, or to be transferred over, the secure connection (that is, message packets other than those for which the external computer, with which the secure connection was established, is the respective source or destination), it will be appreciated that the firewall computer 16 may merely send a notification to either the source or destination, or neither. Alternatively or in addition, the firewall computer 16 may provide a notification to a system administrator. As a further alternative, and the firewall computer 16 may merely log the fact that it had received an unauthorized message packet.

It will be appreciated that a system in accordance with the invention can be constructed in whole or in part from special purpose hardware or a general purpose computer system, or any combination thereof, any portion of which may be controlled by a suitable program. Any program may in whole or in part comprise part of or be stored on the system in a conventional manner, or it may in whole or in part be provided in to the system over a network or other mechanism for transferring

information in a conventional manner. In addition, it will be appreciated that the system may be operated and/or otherwise controlled by means of information provided by an operator using operator input elements (not shown) which may be connected directly to the system or which may transfer the information to the system over a network or other mechanism for transferring information in a conventional manner.

The foregoing description has been limited to a specific embodiment of this invention. It will be apparent, however, that various variations and modifications may be made to the invention, with the attainment of some or all of the advantages of the invention. It is the object of the appended claims to cover these and such other variations and modifications as come within the true spirit and scope of the invention.

What is claimed as new and desired to be secured by Letters Patent of the United States is:

CLAIMS

1. A method of selectively transferring messages between a network and a secure connection comprising the steps of:

A. a message packet receiver step of receiving a message packet to be transferred between the network and a device over a secure connection, the device having an device address, and

B. a message packet transfer step of selectively transferring the message packet over at least one of the network or the secure connection, the message packet transfer step including the step of determining whether to transfer the message packet in relation to the device address and an address in the message packet as received during the message packet receiver step.

2. A method as defined in claim 1 in which the message packet receiver step includes the step of receiving the message packet from the network, the message packet including a destination address, the message packet transfer step including the step of transferring the message packet over the secure connection if the destination address corresponds to the device address of the device, and not transferring the message packet over the secure connection if the destination address does not correspond to the device address.

3. A method as defined in claim 2 in which the message packet includes a data portion including data, the method further including a step of encrypting the data prior to the message packet being transferred over the secure connection.

4. A method as defined in claim 1 in which the message packet receiver step includes the step of receiving the message packet from the secure connection, the message packet including a source address, the message packet transfer step including the step of transferring the message packet over the network if the source address corresponds to the device address of the device, and not transferring the message packet over the network if the source address does not correspond to the device address.

5. A method as defined in claim 4 in which the message packet includes a data portion including data, the method further including the step of decrypting the data prior to transferring over the network.

6. A firewall arrangement for use in connection with a network, the firewall arrangement comprising:

A. a message packet receiver module configured to receive a message packet to be transferred between the network and a device over a secure connection, the device having an device address, and

B. a message packet transfer module configured to selectively transfer the message packet over at least one of the network or the secure connection, the message packet transfer module determining whether to transfer the message packet in relation to the device address and an address in the message packet as received by the message packet receiver module.

7. A firewall arrangement as defined in claim 6 in which the message packet receiver module receives the message packet from the network, the message packet including a destination address, the message packet transfer module being configured to transfer the message packet over the secure connection if the destination address corresponds to the device address of the device, and to not transfer the message packet over the secure connection if the destination address does not correspond to the device address.

8. A firewall arrangement as defined in claim 7 in which the message packet includes a data portion including data, the firewall arrangement further including an encryption module configured to encrypt the data prior to the message packet transfer module transferring the message packet over the secure connection.

9. A firewall arrangement as defined in claim 6 in which the message packet receiver module receives the message packet from the secure connection, the message packet including a source address, the message packet transfer module being configured to

transfer the message packet over the network if the source address corresponds to the device address of the device, and to not transfer the message packet over the network if the source address does not correspond to the device address.

10. A firewall arrangement as defined in claim 4 in which the message packet includes a data portion including data, the firewall arrangement further including a decryption module configured to decrypt the data prior to the message packet transfer module transferring the message packet over the network.

11. A computer program product for use in connection with a computer to form a firewall arrangement for use in connection with a network, the computer program product comprising a computer–readable medium having encoded thereon:

A. a message packet receiver module configured to enable said computer to receive a message packet to be transferred between the network and a device over a secure connection, the device having an device address, and

B. a message packet transfer module configured to enable said computer to selectively transfer the message packet over at least one of the network or the secure connection, the message packet transfer module determining whether to transfer the message packet in relation to the device address and an address in the message packet as received by the message packet receiver module.

12. A computer program product as defined in claim 11 in which the message packet receiver module receives the message packet from the network, the message packet including a destination address, the message packet transfer module being configured to enable said computer to transfer the message packet over the secure connection if the destination address corresponds to the device address of the device, and to not transfer the message packet over the secure connection if the destination address does not correspond to the device address.

13. A computer program product as defined in claim 12 in which the message packet includes a data portion including data, the computer program product further

including an encryption module configured to enable said computer to encrypt the data prior to the message packet transfer module transferring the message packet over the secure connection.

14. A computer program product as defined in claim 11 in which the message packet receiver module receives the message packet from the secure connection, the message packet including a source address, the message packet transfer module being configured to enable said computer to transfer the message packet over the network if the source address corresponds to the device address of the device, and to not transfer the message packet over the network if the source address does not correspond to the device address.

15. A computer program product as defined in claim 14 in which the message packet includes a data portion including data, the computer program product further including a decryption module configured to enable said computer to decrypt the data prior to the message packet transfer module transferring the message packet over the network.

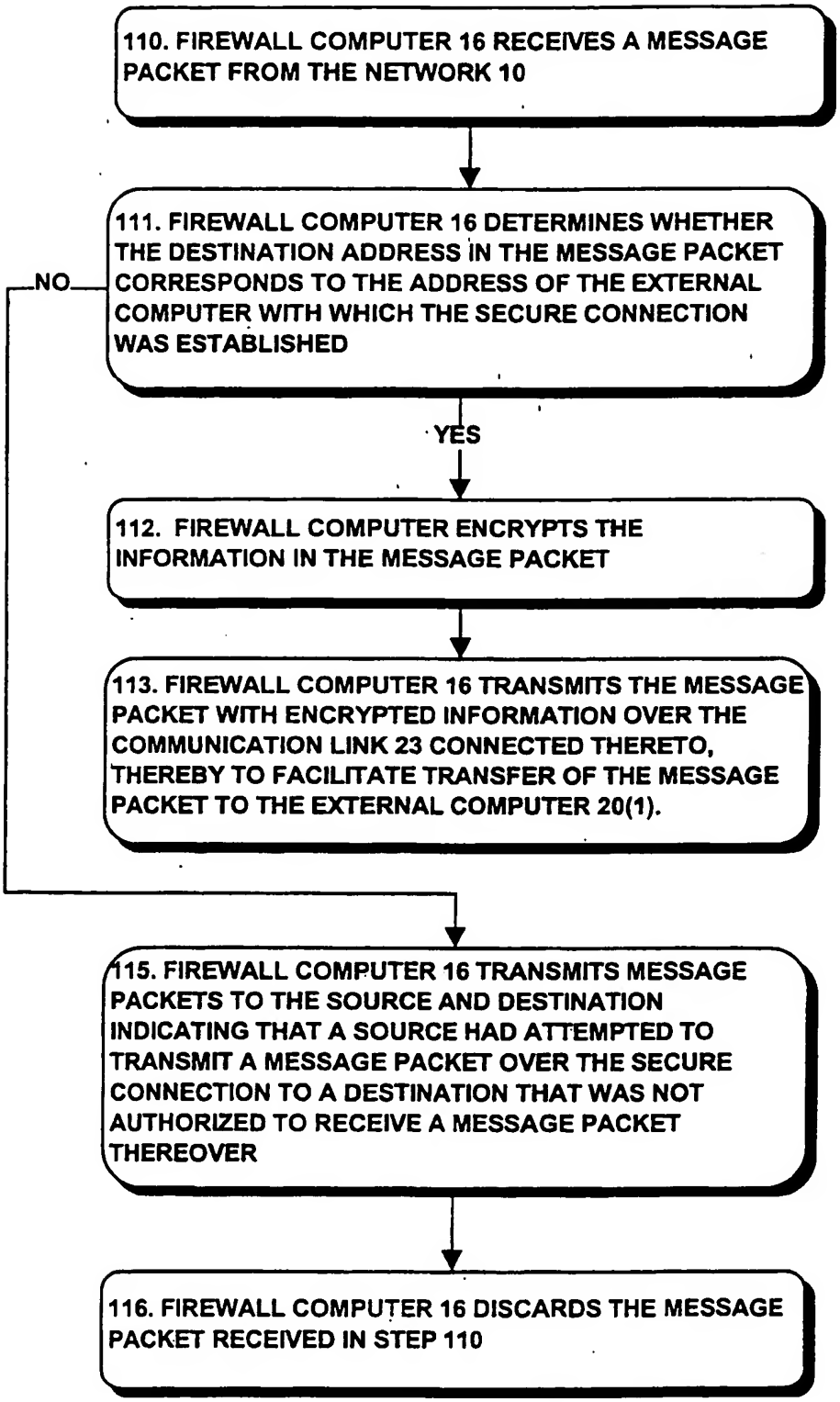

110. FIREWALL COMPUTER 16 RECEIVES A MESSAGE PACKET FROM THE NETWORK 10
111. FIREWALL COMPUTER 16 DETERMINES WHETHER THE DESTINATION ADDRESS IN THE MESSAGE PACKET CORRESPONDS TO THE ADDRESS OF THE EXTERNAL COMPUTER WITH WHICH THE SECURE CONNECTION WAS ESTABLISHED
NO
YES
112. FIREWALL COMPUTER ENCRYPTS THE INFORMATION IN THE MESSAGE PACKET
113. FIREWALL COMPUTER 16 TRANSMITS THE MESSAGE PACKET WITH ENCRYPTED INFORMATION OVER THE COMMUNICATION LINK 23 CONNECTED THERETO, THEREBY TO FACILITATE TRANSFER OF THE MESSAGE PACKET TO THE EXTERNAL COMPUTER 20(1).
115. FIREWALL COMPUTER 16 TRANSMITS MESSAGE PACKETS TO THE SOURCE AND DESTINATION INDICATING THAT A SOURCE HAD ATTEMPTED TO TRANSMIT A MESSAGE PACKET OVER THE SECURE CONNECTION TO A DESTINATION THAT WAS NOT AUTHORIZED TO RECEIVE A MESSAGE PACKET THEREOVER
116. FIREWALL COMPUTER 16 DISCARDS THE MESSAGE PACKET RECEIVED IN STEP 110

FIG. 3

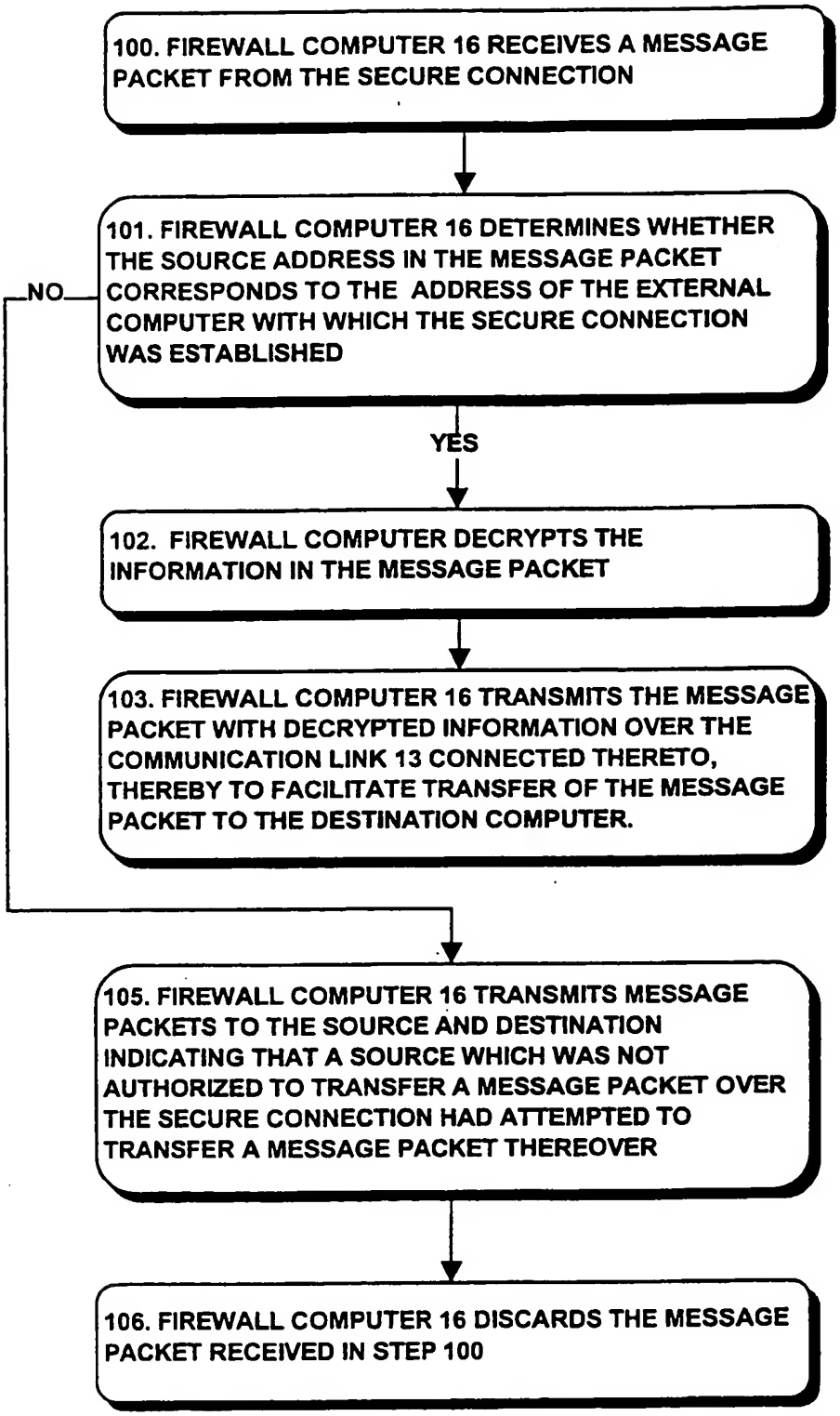

100. FIREWALL COMPUTER 16 RECEIVES A MESSAGE PACKET FROM THE SECURE CONNECTION
101. FIREWALL COMPUTER 16 DETERMINES WHETHER THE SOURCE ADDRESS IN THE MESSAGE PACKET CORRESPONDS TO THE ADDRESS OF THE EXTERNAL COMPUTER WITH WHICH THE SECURE CONNECTION WAS ESTABLISHED
NO
YES
102. FIREWALL COMPUTER DECRYPTS THE INFORMATION IN THE MESSAGE PACKET
103. FIREWALL COMPUTER 16 TRANSMITS THE MESSAGE PACKET WITH DECRYPTED INFORMATION OVER THE COMMUNICATION LINK 13 CONNECTED THERETO, THEREBY TO FACILITATE TRANSFER OF THE MESSAGE PACKET TO THE DESTINATION COMPUTER.
105. FIREWALL COMPUTER 16 TRANSMITS MESSAGE PACKETS TO THE SOURCE AND DESTINATION INDICATING THAT A SOURCE WHICH WAS NOT AUTHORIZED TO TRANSFER A MESSAGE PACKET OVER THE SECURE CONNECTION HAD ATTEMPTED TO TRANSFER A MESSAGE PACKET THEREOVER
106. FIREWALL COMPUTER 16 DISCARDS THE MESSAGE PACKET RECEIVED IN STEP 100

FIG. 2

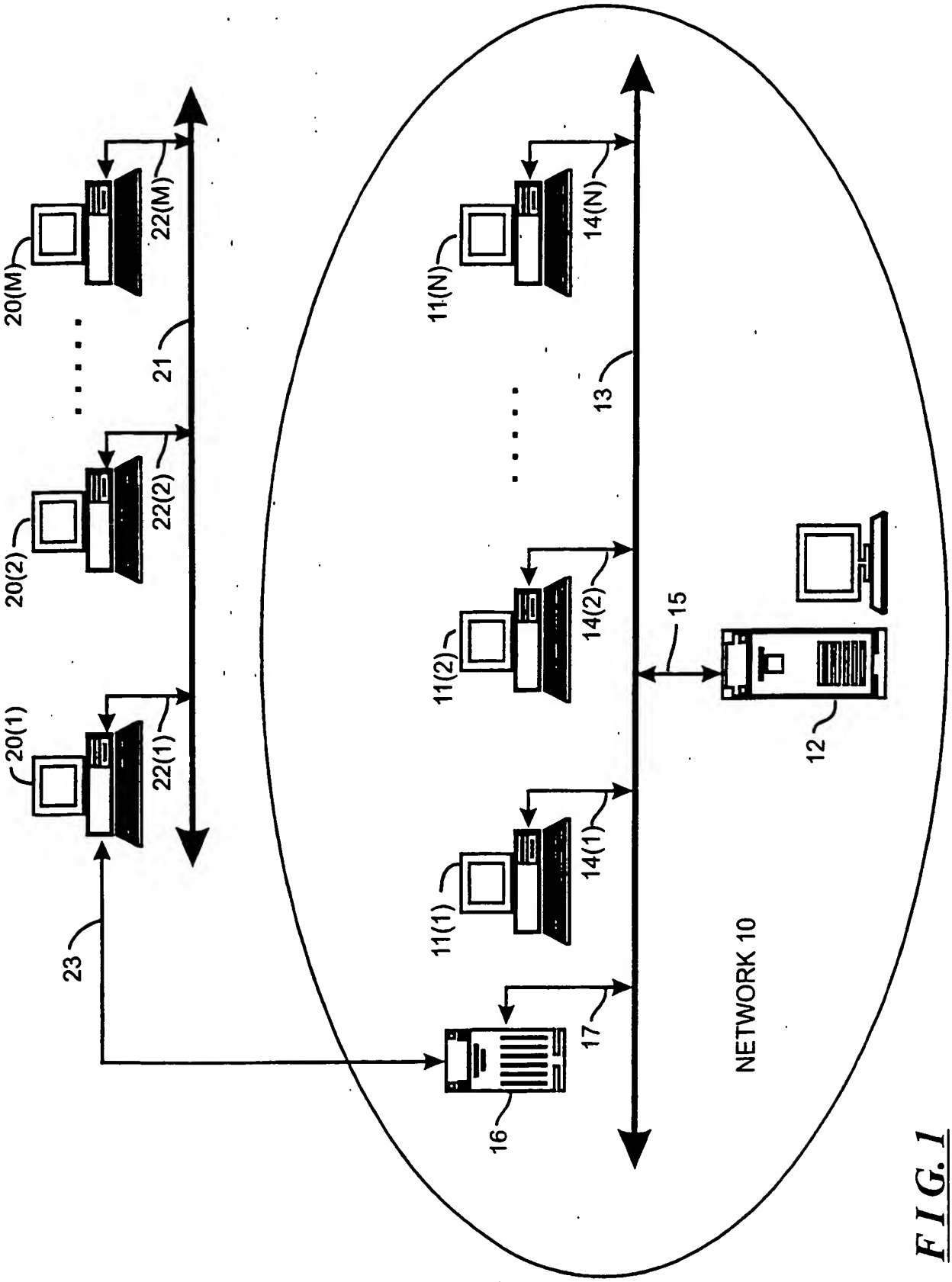

20(M)
22(M)
21
20(2)
22(2)
20(1)
22(1)
23
11(N)
14(N)
13
11(2)
14(2)
15
12
11(1)
14(1)
17
16
NETWORK 10

FIG. 1